УДК 004.056

А.И. СТРЕЛЕЦ, М.Н. ЁХИН, И.А. ЛОГВИНЕНКО
Национальный исследовательский ядерный университет «МИФИ», Москва

АУТЕНТИФИКАЦИЯ И АВТОРИЗАЦИЯ ЦИФРОВЫХ УСТРОЙСТВ В МНОГОПОЛЬЗОВАТЕЛЬСКОЙСИСТЕМЕ ВИРТУАЛЬНЫХ СТЕНДОВ

В современных информационных и вычислительных системах проблеме аутентификации пользователя отведено важное место и существует целый ряд решений, обеспечивающих безопасную аутентификацию. Однако большинство этих способов аутентификации предполагают, что субъектом аутентификации являются люди. В системе виртуальных стендов, предназначенной для многопользовательской удаленной работы студентов и преподавателей с различными цифровыми устройствами, субъектами аутентификации выступают не только люди, но и цифровые устройства – FPGA, SoC и др. При этом, уровень развития средств информационной безопасности в решениях производителей цифровых устройств либо низок, либо такие средства отсутствуют вовсе. Это приводит к необходимости разработки средств аутентификации и авторизации, предназначенных для работы с цифровыми устройствами.

Современные информационные и вычислительные системы отличаются высокой архитектурной сложностью и обилием составных компонентов. Всё это увеличивает объем оборудования системы, доступного злоумышленнику для атаки. Наиболее простой способ защиты от атаки – это физическая недоступность системы из сети интернет. В случае с рабочими местами пользователей в лаборатории именно изолированность служит самой надежной защитой, поскольку вся работа происходит в локальном режиме на компьютерах в лаборатории. Пользователю доступен компьютер на рабочем месте, цифровое устройство подключено к компьютеру через USB, а доступ в интернет осуществляется через стандартные порты или отсутствует вовсе. Проблема защищенности рабочего места в такой конфигурации эквивалентна проблеме защищенности обычного рабочего места пользователя и имеет массу стандартных решений [1]. Иначе обстоит дело, если возникает необходимость удаленного доступа к цифровым устройствам в лаборатории.

Учебный процесс в лабораториях с цифровыми устройствами выстроен таким образом, что пользователи (студенты) используют цифровые устройства, установленные в лаборатории. Это накладывает

ограничения на образовательный процесс, делая невозможным удаленные курсы или доступ в нерабочее время. Для решения этой проблемы была разработана многопользовательская система со специальными виртуальными стендами для удаленного подключения студентов к устройствам через интернет. Однако использование этой системы привело к возникновению дополнительных векторов атаки через сеть. Система является веб-сервисом, к которому подключаются студенты, преподаватели, а также цифровые устройства. Аутентификация пользователей осуществляется стандартными средствами на основе пароля. Помимо людей, к данной системе также подключаются и обмениваются информацией устройства из лаборатории. Эти устройства также являются субъектами аутентификации, не являясь при этом людьми. Стандартные средства аутентификации – аутентификация на основе пароля, двухфакторная аутентификация или на основе токенов не являются применимыми в данном случае, поскольку подразумевают использование пароля, который необходимо хранить отдельно от устройства [2].

Наиболее перспективным способ аутентификации устройств в данном случае является аутентификация на основе ключей доступа. Такой подход позволяет избежать передачи пароля сторонний приложениям или злоумышленнику [3]. Однако, тот факт, что субъектом аутентификации является устройство, а не пользователь, добавляет свои особенности. Например, ключ может храниться внутри устройства в специальных разделах памяти на FPGA.

Таким образом, актуальной задачей является разработка способа аутентификации на основе ключей доступа для случаев, когда субъектом аутентификации являются цифровые устройства лаборатории, и интеграция этого способа аутентификации в многопользовательскую систему виртуальных стендов.

Список литературы

1. Ричард Э. Смит. Аутентификация: от паролей до открытых ключей. Authentication: From Passwords to Public Keys First Edition. – М.: Вильямс, 2002. – 432 с.

2. Шнайер Б.Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Applied Cryptography. Protocols, Algorithms and Source Code in C. – М.: Триумф, 2002. – 816 с.

3. Иванов М.А. Способ обеспечения универсальной защиты информации, пересылаемой по каналу связи. // Вопросы кибербезопасности. – 2019. – № 3(31). – С. 45–50. DOI: 10.21681/2311-3456-2019-3-45-50.